COMPETITIVE INTELLIGENCE
& STRATEGY

QKS Group

Security and Risk Management

SPARK Matrix™ : Connected Medical Device Security Solution, 2024

September 2024

Mohnish Rathore

Sofia Ali

TABLE OF CONTENTS

Executive Overview

This research service includes a detailed analysis of the global Connected Medical Device Security Solution market dynamic, vendor landscape, and competitive positioning analysis. The study provides a competitive analysis of leading vendors. This research provides strategic information for technology vendors to better understand the market supporting their growth strategies and for users to evaluate different vendors' capabilities and competitive differentiation.

Market Dynamics and Overview

QKS Group defines Connected Medical Device Security (CMDS) solution as" a comprehensive solution designed to protect networked medical devices from cyber threats." These solutions identify, track, and secure all medical devices in Healthcare Delivery Organizations (HDOs) against vulnerabilities and breaches. The solution's key capabilities include real-time monitoring, threat detection, vulnerability management, compliance enforcement, and device analytics. The solutions protect Internet of Medical Things (IoMT) devices, networks, building management systems, and other connected devices, besides providing asset visibility and risk management. This protection ensures the safety, privacy, and operational integrity of medical devices, secured sensitive patient data, and continuous, reliable operation of critical medical equipment."

Healthcare delivery entities (HDOs) such as hospitals and clinics must manage complex networks that include Internet of Medical Things (IoMT), Operational Technology (OT), and Internet of Things (IoT) devices. The increasing use of IoMT is crucial in the field of Medical Technology (MedTech), but these devices are vulnerable to threats like ransomware, which can lead to severe consequences, including human fatalities. However, securing interconnected medical devices is a challenging process due to their proprietary protocols and the sheer number of devices, making inventory management difficult for HDOs. These challenges highlight the need for Connected Medical Device Security (CMDS) solutions.

CMDS solutions protect IoT, OT, IT, and edge assets within the HDO ecosystem from attacks, threats, and data exfiltration attempts. These solutions streamline automated asset management, providing a comprehensive approach to locating, identifying, tracking, and monitoring all connected assets, whether managed or unmanaged. This streamlined process reduces costs and enhances the financial performance of HDOs. CMDS solutions offer extensive network visibility, allowing administrators to supervise equipment, improve security posture, optimize inventory and staffing, and ensure regulatory compliance.

The following is a detailed description of the key capabilities of a connected medical device security solution:

- **Asset Inventory Management:** This capability helps the HDOs to accurately map and categorize devices connected to their networks. It also enables HDOs to identify and monitor both managed and unmanaged clinical and non-clinical devices across their diverse network ecosystem. It provides real-time,

comprehensive insight into the network, including connections to unauthorized or unmanaged networks, updates inventory levels, and streamlines inventory management, resulting in significant cost savings. This capability also leverages data from the FDA database to identify recalls and obtain classification, version, and risk information from manufacturer databases.

- **Risk Management:** This key capability helps alleviate the concerns about the clinical hazards associated with devices, such as PHI transmission volume and ongoing FDA recalls. It identifies risks or irregularities and initiates protective protocols to minimize potential hazards. The solution evaluates all inventory items for cybersecurity vulnerabilities, providing a risk score that helps the information security team strategize to minimize potential issues. The risk management plan includes tasks like implementing firmware upgrades, updating operating systems, altering communication protocols, applying vendor patches, and proposing network segmentation.

- **Vulnerability Management:** Most medical devices rely on firmware, which can become outdated over time. A medical device security solution includes a vulnerability management module to ensure comprehensive patching. This module identifies and resolves vulnerabilities in devices that cannot be patched due to regulatory constraints or specific model versions, protecting the HDO network from potential access points for attackers.

- **Compliance with Medical Regulations:** The medical device security solution ensures compliance with medical regulations and directives related to data transmission and personal information security. It simplifies audit mechanisms for HDOs by ensuring compliance with regulations such as HIPAA, PII, and PCI-DSS. Additionally, it provides compliance reports and audit trials to meet regulations.

- **Policy Management:** The policy management feature allows administrators to define and monitor policies for automatically mitigating risks or addressing security incidents. This capability enables HDOs to create custom protocols for addressing policy breaches, define exemptions, run network segmentation policies, and adjust sensitivity levels based on device characteristics and risk evaluations.

- **Device Analytics & Dashboard Reporting:** The connected medical device security solution offers integrated analytics and reporting features that monitor all device actions, construct dashboards, and produce reports. Device analytics provide operational insights regarding device usage, helping HDO administration optimize device quantities and reduce costs by highlighting underutilized

equipment. Reports offer valuable information on security status, identified risks, vulnerabilities, inventory quantities, device usage, and maintenance notifications. These reports are integrated into security or network operation centers and biomedical engineering workplaces and can be presented through a centralized dashboard for real-time operational details.

- **Event Detection and Response:** The event detection and response capability use risk analysis results to monitor operations around medical devices, managing identified risks. Upon detecting a risk, the capability generates an event alert, providing comprehensive information to create an organizational response.

- **Network Monitoring:** The network monitoring feature oversees all devices and entry points within the HDO network, identifying vulnerable points, compromised devices, data leakage, anomalies, breaches, or any behavior posing a risk to device security or violating regulations such as HIPAA or PII. This includes activities like data extraction attempts, phishing attempts, malware and ransomware incidents, direct manipulation of medical device controls, or unauthorized access to sensitive medical records. The capability includes packet sniffing and packet capture features for in-depth packet analysis in case of an attack.

- **Scalability and Deployment Options:** Healthcare Delivery Organizations (HDOs) should prioritize vendors that offer flexible deployment options, including on-premises, cloud-based, and hybrid solutions, to accommodate various organizational needs. Additionally, the solution should ensure scalability, allowing it to grow alongside the organization by supporting an increasing number of devices and expanding network infrastructure. This flexibility and scalability ensure that the solution remains effective and efficient as the HDO's technological landscape evolves.

Competitive Landscape and Analysis

QKS Group conducted an in-depth analysis of the major connected medical device security solution vendors by evaluating their products, market presence, and value proposition. The evaluation is based on primary research with expert interviews, analysis of use cases, and QKS Group's internal analysis of the overall connected medical device security solutions market. This study includes an analysis of key vendors, including AirEye, Armis, Asimily, Claroty, CloudWave, Cybeats, Cylera, Cynerio, Forescout, Gurucul, Ordr, Palo Alto Networks, and Sepio.

Armis, Claroty, CloudWave, Cylera, Cynerio, and Sepio are the top performers and leaders in the global Connected Medical Device Security solutions market. These companies offer a sophisticated and comprehensive technology platform that provides visibility, location tracking, usage monitoring, and risk scoring for all devices within the network ecosystem. The platform categorizes devices based on their type, criticality, and associated risk, maintaining real-time updates of device inventory. It secures devices from various types of threats by performing risk analysis and providing remediation based on the criticality and risk level of each device. Additionally, the platform enhances efficiency by identifying underutilized devices within the network ecosystem.

Armis Centrix™ platform provides a range of capabilities. These include real-time, comprehensive visibility into the inventory of medical devices, insights into device usage for optimizing efficiency, risk assessments based on device vulnerabilities, detection of breaches involving Protected Health Information (PHI), identification of threats along with their remediation, and the automation of medical device security.

Claroty offers Medigate, a SaaS-powered healthcare cybersecurity platform designed to secure organizational device ecosystems while meeting business objectives. The platform enables HDOs to effectively monitor and mitigate risks within their Extended Internet of Things (XIoT) landscape.

CloudWave's SensatoMD solution is a comprehensive single-suite solution for medical devices. This solution includes features such as medical device vulnerability assessment, a breach detection system through the Sensato Cybersecurity-as-a-Service platform, and guidance for incident response related to medical devices.

Cylera's Cylera Platform takes a proactive approach to managing connected medical devices within an organization's network ecosystem. The comprehensive platform includes features such as Executive Management, Procurement & Vendor Management,

Information Security, Risk Management & Compliance, and Information Technology. These features provide HDOs enhanced control over devices, enabling improved operational efficiency and security measures. The platform aids the IT teams in monitoring and managing network devices, offering in-depth insights that optimize device maintenance and management practices.

Cynerio offers the Cynerio Platform, which enables HDOs to detect and address threats associated with medical devices within the network, including IoMT, IoT, OT, unmanaged IT, and mobile devices. The company's Healthcare IoT Attack Detection and Response solution allows HDOs to identify and mitigate threats originating from these devices. Additionally, Cynerio's Preventative Risk Management solution provides insights into the interconnected medical devices, IoT, and OT infrastructure.

Sepio's Asset Risk Management platform provides device security features for Healthcare Delivery Organizations (HDOs). This platform ensures complete asset visibility, regardless of location, type, or usage, and offers integration with third-party vendors. It also helps achieve compliance with global regulations such as HIPAA and GDPR.

AirEye, Asimily, Forescout, Gurucul, Ordr, and Palo Alto Networks have been positioned as strong contenders. The AirEye solution offers a range of features, including monitoring wireless channels, identifying and classifying assets, categorizing devices and networks, detecting breaches, quickly terminating attacks, and providing forensic insights. The company offers two deployment options. The first option uses an Overlay Architecture with strategically placed software-based sensors called "Halo," which eliminates the need for an endpoint agent. The second option integrates the AirEye solution with the cloud by connecting the AirEye server to the Cisco Meraki cloud network using an API key, enhancing the solution's scalability.

Asimily provides the Asimily Risk Remediation Platform, which includes features such as device identification and documentation, inventory record maintenance, network activity monitoring, risk identification and mitigation, threat and vulnerability management, policy management, and the use of analysis and reporting tools.

Forescout's Forescout Platform continuously ensures compliance across various cyber assets, including IT, IoT, IoMT, and OT, while minimizing business disruptions. Forescout eyeSight provides comprehensive visibility into all devices within the extended enterprise, detecting and categorizing all IP-connected devices and promptly assessing their compliance status and risks. Forescout Risk and Exposure Management tool helps organizations understand the security posture of potential targets. Additionally, Forescout eyeSegment simplifies the creation, planning, and implementation of adaptable, non-intrusive segmentation for all cyber assets.

Gurucul's security solution for connected medical devices includes key functions such as device recognition, continuous monitoring, inventory management, risk evaluation, vulnerability control, compliance monitoring, and robust analytics with reporting options. The company enhances its offering with a managed security analytics service. Additionally, Gurucul's UEBA can identify a device deviating from its regular operational cycle and determine the optimal time for maintenance, such as patching.

Ordr offers comprehensive security solutions for connected medical devices through its OrdrAI Asset Intelligence Platform. This platform includes features such as asset discovery, classification, and tracking; vulnerability and risk management; threat detection and mitigation; compliance management; Zero Trust micro-segmentation; NAC implementation; and advanced reporting tools. It is designed to enhance visibility, identify and protect all connected devices, and simplify the protection of the connected business environment.

Palo Alto's Medical IoT Security solution allows enterprises to identify and assess all connected devices within their network. The solution facilitates device segregation and enforces the principle of least privilege access, ensuring continuous protection of medical devices against cyber threats.

Cybeats has been placed as an aspirant in the Connected Medical Device Security market. Cybeats' RDSP IoT Security Platform features a dashboard that integrates with SIEM systems to aid Security Operation Centers in rapidly responding to attacks. The dashboard provides visibility of devices within the ecosystem and delivers threat intelligence to identify emerging threats.

All the vendors captured in the 2024 SPARK Matrix™ of Connected Medical Device Security vendors are focusing on enhancing their ability to identify all devices within the network ecosystem, conducting risk assessments, and providing accurate risk scores. They aim to increase the operational efficiency of these devices and simplify compliance with global regulations. Organizations are continually improving their Connected Medical Device Security products and expanding support for multiple deployment options.

Key Competitive Factors and Technology Differentiators

Many connected medical device security solution vendors provide comprehensive functionalities that support different use cases. However, their technology and customer value proposition may differ depending on customer size, industry vertical, geographic location, and organization-specific needs. Some of the key competitive technology differentiators for an integrated connected medical device security solution are:

- **Network Segmentation:** Healthcare delivery organizations should prioritize vendors that adopt network segmentation as a strategic approach to address various IT and IoMT (Internet of Medical Things) challenges. This method offers numerous advantages, such as enhanced security by preventing the spread of threats across the network, controlling access to critical patient data to mitigate data exfiltration risks, and reducing the attack surface for essential functions performed by vulnerable medical systems.

- **Knowledge Repositories:** Users should seek vendors that provide proprietary knowledge repositories containing extensive data on medical devices, including their attack history and patterns. These repositories enable solutions to identify, categorize, and integrate a wide range of medical devices from different manufacturers and versions. Furthermore, they aid in detecting attacks and vulnerabilities, allowing for the identification of optimal remedial actions through historical data analysis, thereby reducing Mean Time to Remediation (MTTR).

- **Use of AI/ML:** Organizations should consider vendors that utilize artificial intelligence (AI) and machine learning (ML) in their tools for managing vulnerabilities and reporting. Some vendors offer the capability to detect vulnerabilities by analyzing a device's Software Bill-of-Materials (SBOM). This integration allows Healthcare Delivery Organizations (HDOs) to proactively establish measures for vulnerability mitigation before potential incidents occur.

- **Service Delivery models:** Organizations should look for vendors that provide agentless passive real-time monitoring to save the time and effort required for maintenance and updates. Most medical devices are not compatible with agent-based solutions, and active monitoring tools could disrupt their essential functions. Vendors should offer a variety of deployment options. Depending on their specific

needs, HDOs can choose vendors that provide their preferred deployment model, whether on-premises or in the cloud.

- **Integration, Interoperability, and Ease of Use:** Users should look for vendors with established technological collaborations with other security providers or those offering comprehensive integrations. These integrations facilitate the smooth incorporation of solutions into the HDO's existing security framework, including systems like Security Information and Event Management (SIEM) or Network Access Control (NAC), network infrastructure solutions, third-party risk management databases, and analytical tools. Such integrations help organizations understand their device ecosystem and security levels.

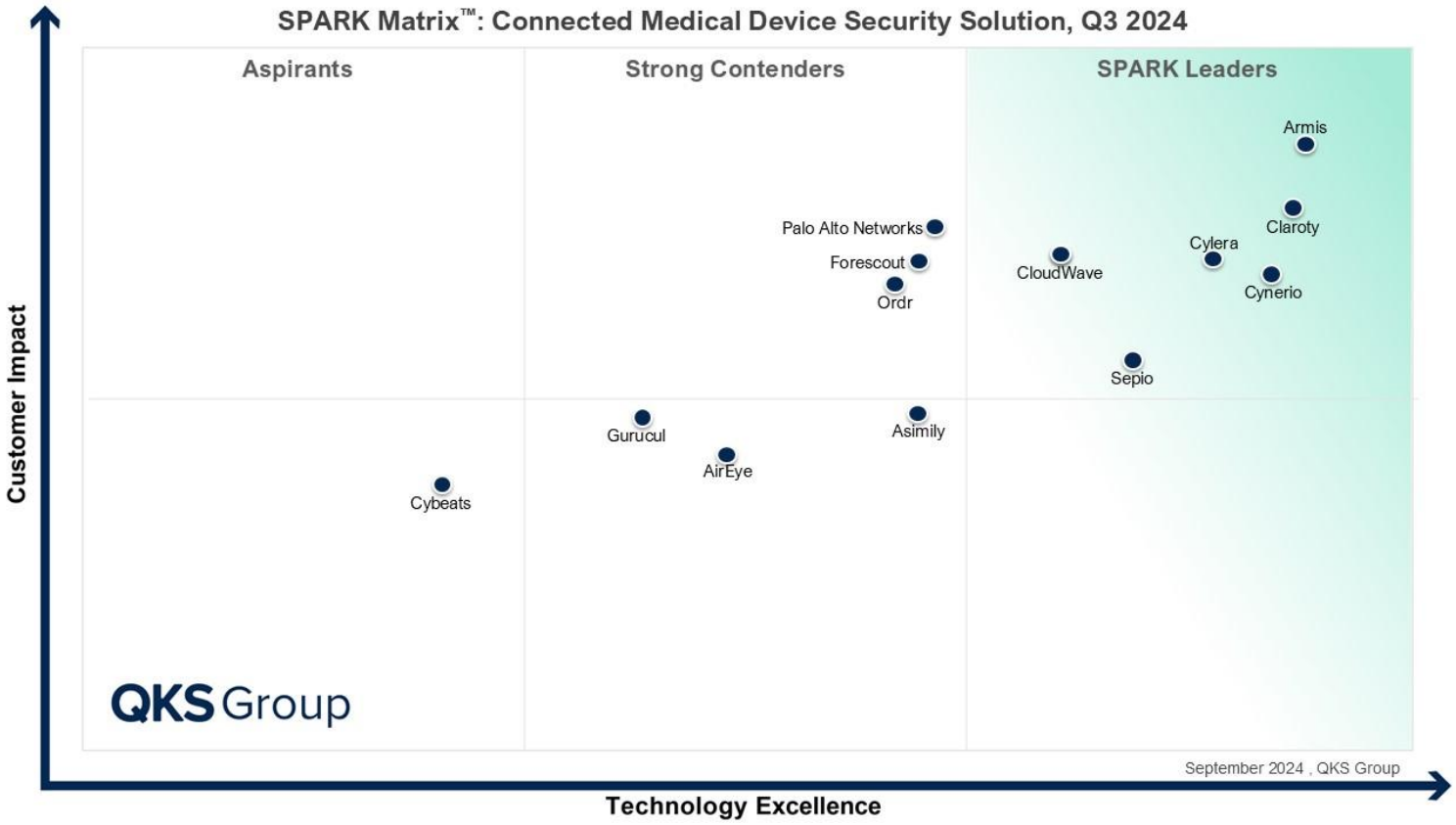
- **User Experience and Interface:** Users should seek vendors that provide intuitive and user-friendly interfaces to simplify the management and monitoring of connected medical devices. Vendors should offer comprehensive dashboards and reporting tools that deliver clear and actionable insights, ensuring that HDOs can effectively oversee their device ecosystem and make informed security decisions.

SPARK Matrix™: Connected Medical Device Security

Strategic Performance Assessment and Ranking

Figure: 2024 SPARK Matrix™

(Strategic Performance Assessment and Ranking)
Connected Medical Device Security Solution Providers



Vendor Profile

Following are the profiles of the leading Connected Medical Device Security solution vendors with a global impact. The following vendor profiles are written based on the information provided by the vendor's executives as part of the research process. QKS Group research team has also referred to the company's website, whitepapers, blogs, and other sources for writing the profile. A detailed vendor profile and analysis of all the vendors, along with various competitive scenarios, are available as a custom research deliverable to our clients. Users are advised to directly speak to respective vendors for a more comprehensive understanding of their technology capabilities. Users are advised to consult QKS Group before making any purchase decisions regarding connected medical device security solution and vendor selection based on research findings included in this research service.

Armis

URL: https://www.armis.com/

Founded in 2015 and headquartered in San Francisco, California, USA, Armis offers a cyber exposure management platform, Armis Centrix™, that sees, protects, and manages critical assets in real-time for IT, cloud, IoT devices, medical devices (IoMT), operational technology (OT), industrial control systems (ICS), and 5G environments. Armis Centrix™ for Medical Device Security provides complete visibility, continuous security, and optimized utilization of IoMT, unmanaged medical/non-medical devices.

The Armis Centrix™ platform offers real-time comprehensive visibility, security, and control of medical device inventory, detailed contextual insights into device usage to enhance utilization efficiency, and medical device risk assessment and remediation based on identified vulnerabilities and other security issues. It also detects Protected Health Information (PHI) breaches, identifies and mitigates threats, and automates the security of medical devices. The product is equipped with an Asset Intelligence Engine that utilizes the AI-powered Armis Standard Query for advanced data analysis.

Analyst Perspective

Key Differentiators

- Armis' AI-driven Asset Intelligence Engine leverages a multi-discipline detection engine with a proprietary database of over 5 billion asset profiles to provide comprehensive situational awareness for all assets and devices. It integrates with IT and security solutions for complete inventory and utilizes a multi-detection engine that delivers both passive and smart active querying, which can be set by the administrator
- The Armis Centrix™ platform offers a unified approach to technology risk prioritization and resolution lifecycle management across code, infrastructure, cloud, and application findings. Armis Centrix™ for Medical Device Security utilizes a data-centric, AI-driven methodology to enable the security stakeholders to track device utilization and better identify and manage medical risks such as FDA Recalls/MDS2.
- Armis Centrix™ for Actionable Threat Intelligence is an Artificial Intelligence (AI) and machine learning-powered early warning system. This system empowers customers with early warning intelligence, enabling them to anticipate threats, understand their potential impact, and take preemptive action to neutralize them. By moving the security posture from defense to offense, this solution helps organizations stay proactive in their security measures.

- The platform offers a wide range of reports and dashboards for quick data analysis and provides a flexible search query with natural language capabilities. This wide selection allows users to search for any asset or attribute they need. The search functionality is comprehensive and enables deep-level queries without the need for additional development work.

- With visibility into over 5 billion assets worldwide, Armis claims to offer superior asset intelligence in real-time based on its ability to track expected vs. actual behaviors of systems and assets. This capability allows organizations to maintain a current and accurate real-time assessment of all connected devices, ensuring proactive security management.

Product Strategy

- **Technology Roadmap**: Armis' technology roadmap is focused on several key areas as part of its healthcare cybersecurity security suite. This suite includes Armis Centrix™ for Medical Device Security, Armis Centrix™ for Actionable Threat Intelligence, and Armis Centrix™ for VIPR – Prioritization and Remediation to streamline workflows stemming from security findings, as well as developing an Intelligence Center for Healthcare to provide peer-comparison and recommendations to help organizations improve their security posture. Furthermore, Armis' strategy also focuses on reducing risk and cost for healthcare delivery organizations (HDOs) with enhancements including device lifecycle management, cyber protection and resilience, operational/clinical efficiency, and compliance with the changing healthcare regulatory landscape. With this intersection of clinical care, cybersecurity, and AI, Armis' strategy is focused on prioritizing and mitigating risk impacting patient care services, to improve security posture, reduce costs, and ultimately minimize any disruption to patient care.

- **Strategic Roadmap**: Armis continues to innovate and deliver on its long-term vision to provide customers with the capabilities they need to manage the entire lifecycle from early warning of potential attacks to full visibility of the entire attack surface, intelligent prioritization, and effective remediation. It plans to further advance the Armis Centrix™ Platform, by investing heavily in R&D and evaluating potential acquisitions, to expand its product suites and effectively leverage AI to predict and address threats, whether physical or virtual.

Market Strategy

- **Geo-expansion Strategy**: Armis will continue its expansion in North America, EMEA, the Middle East, and Asia Pacific.

- **Industry Strategy**: Armis continues to grow its customer base in the healthcare, public, finance, logistics, manufacturing, retail, transportation, and education sectors.

- **Use Case Support**: Armis Centrix™ for Medical Device Security encompasses various use cases to enhance the visibility, security, and operational efficiency of healthcare devices like asset inventory, real-time monitoring, and threat detection. The platform supports data-driven purchasing decisions and operational optimization with detailed utilization analytics. It also provides robust network segmentation to minimize attack surfaces and ensures compliance by integrating with regulatory bodies, identifying affected devices, and following up on recalls. Armis continuously updates its compliance and security frameworks to meet evolving healthcare standards.

Customer/ User Success Strategy

- Armis Centrix™ is a SaaS solution that provides visibility, compliance, risk, and vulnerability management from the cloud. Optional on-prem collectors and solutions are available for network telemetry and local integrations.

- Armis offers pre-defined value packs for fast time to value, featuring customized policies, dashboards, and reports. The platform excels in threat detection with AI-based early warnings, smart honeypots, deception technologies, and malware/ransomware protection. Supported by a dedicated customer success team of over 100 healthcare-experienced members, Armis also fosters a collaborative community for sharing best practices among users and partners.

- Armis has established strategic partnerships to enhance its medical device security solutions. These include Fortinet's suite, Nuvolo's Dynamic CMBD updates, ServiceNow's Service Graph Connector, Cisco's ISE and WLC for simplified segmentation, and TRIMEDX's clinical engineering solution. Additionally, the platform is available in AWS and GCP marketplaces, enhancing its accessibility and integration capabilities. Armis collaborates with the largest global system integrators, including PWC, Accenture, and KPMG, as well as healthcare-dedicated integrators like Fortified Health, Trimedx, and Cyber Salus.

Trend Analysis

- The medical device security market is evolving towards expanded device coverage, including IoT and OT, enhanced vulnerability management, workflow automation, and zero-trust strategies.

- Armis excels in medical device security by providing coverage of IT, OT, IoT, and IoMT devices from ground to cloud, thus enhancing visibility by eliminating blind spots and integrating with the organization’s existing security stack. It focuses on vulnerability management, workflow automation, and advanced threat detection. Through strategic

acquisitions and partnerships, Armis streamlines monitoring, remediation, and incident response staying ahead with proactive threat intelligence and security improvements.

Final Take

- Armis Centrix™ for Medical Device Security provides comprehensive visibility, security, and manageability into all connected devices across healthcare environments, including IT, IoT, OT, and medical devices. It delivers real-time, uninterrupted device discovery and in-depth risk assessments by identifying vulnerabilities and risk and integrating with existing tools. Armis Centrix™ supports inventory management, monitoring device utilization, and ensuring operational efficiency. It also offers advanced threat detection and vulnerability management through automation and integration with various regulatory and security frameworks and requirements. The platform enhances security posture by leveraging extensive partnerships and unique features like vulnerability prioritization and remediation that extend beyond just vulnerabilities to all security findings for streamlined remediation and response.
- Users looking for an easy-to-use Connected Medical Device Security solution with a strong customer base in North America and EMEA regions, offering various use cases in industry verticals such as healthcare can choose the Armis Centrix™ solution.

SPARK Matrix™: Strategic Performance Assessment and Ranking

QKS Group' SPARK Matrix™ provides a snapshot of the market positioning of the key market participants. SPARK Matrix™ provides a visual representation of market participants and provides strategic insights on how each supplier ranks related to their competitors concerning various performance parameters based on the category of technology excellence and customer impact. QKS Group's Competitive Landscape Analysis is a useful planning guide for strategic decision-making, such as finding M&A prospects, partnerships, geographical expansion, portfolio expansion, and similar others.

Each market participant is analyzed against several parameters of Technology Excellence and Customer Impact. In each of the parameters (see charts), an index is assigned to each supplier from 1 (lowest) to 10 (highest). These ratings are designated to each market participant based on the research findings. Based on the individual participant ratings, X and Y coordinate values are calculated. These coordinates are finally used to make SPARK Matrix™.

Technology Excellence	Weightage
Device Discovery and management	15%
Risk Analytics and Management	15%
Analytics	15%
Technology Differentiators	15%
Vulnerability management	10%
Threat Response and Management	10%
Dashboarding, Reporting, and Compliance	10%
Vision & Roadmap	10%

Customer Impact	Weightage
Product Strategy & Performance	20%
Market Presence	20%
Proven Record	15%
Customer Service Excellence	15%
Unique Value Proposition	15%
Ease of Deployment & Use	15%

Evaluation Criteria: Technology Excellence

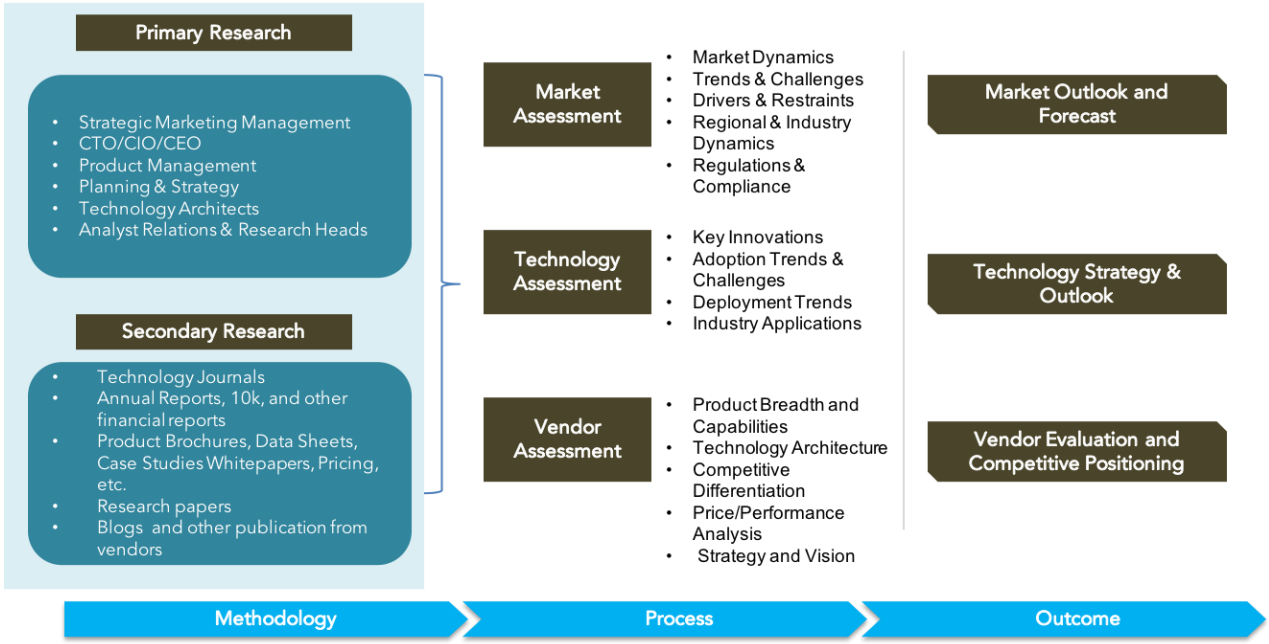
- **Device Discovery and management**: The ability to map and classify devices and identify the real-time location and accurate number of inventories of all medical devices present in the organization.
- **Risk Analytics and Management:** The ability to analyze all devices for risk vulnerabilities and provide a risk score so that organizations can make mitigation plans accordingly.
- **Analytics:** The ability to track usage of devices to optimize the use of underutilized medical devices.
- **Technology Differentiators:** Technical USPs and their competitive advantage.
- **Vulnerability management**: The ability to identify and rectify vulnerabilities associated with medical devices.
- **Threat Response and Management**: The ability to notify threats and communicate information to an organization.
- **Dashboarding, Reporting, and Compliance**: The ability to display the information collected and provide compliance reports for Government regulations.
- **Vision & Roadmap**: Key Planned enhancement to offer superior products/technology.

Evaluation Criteria: Customer Impact

- **Product Strategy & Performance**: Evaluation of multiple aspects of product strategy and performance in terms of product availability, price-to-performance ratio, excellence in GTM strategy, and other product-specific parameters.
- **Market Presence**: The ability to demonstrate revenue, client base, and market growth along with a presence in various geographical regions and industry verticals.
- **Proven Record**: Evaluation of the existing client base from SMB, mid-market, and large enterprise segments, growth rate, and analysis of the customer case studies.
- **Ease of Deployment & Use**: The ability to provide superior deployment experience to clients supporting flexible deployment or demonstrate superior purchase, implementation, and usage experience. Additionally, vendors' products are analyzed to offer a user-friendly UI and ownership experience.
- **Customer Service Excellence**: The ability to demonstrate vendors' capability to provide a range of professional services from consulting, training, and support. Additionally, the company's service partner strategy or system integration capability across geographical regions is also considered.
- **Unique Value Proposition**: The ability to demonstrate unique differentiators driven by ongoing industry trends, industry convergence, technology innovation, and such others.

Research Methodologies

QKS Group uses a comprehensive approach to conduct global market outlook research for various technologies. QKS Group's research approach provides our analysts with the most effective framework to identify market and technology trends and helps in formulating meaningful growth strategies for our clients. All the sections of our research report are prepared with a considerable amount of time and thought process before moving on to the next step. The following is a brief description of the major sections of our research methodologies.



Secondary Research

The following are the major sources of information for conducting secondary research:

QKS Group's Internal Database

QKS Group maintains a proprietary database in several technology marketplaces. This database provides our analyst with an adequate foundation to kick-start the research project. This database includes information from the following sources:

- Annual reports and other financial reports
- Industry participant lists

- Published secondary data on companies and their products.
- Major market and technology trends

Literature Research

QKS Group leverages several magazine subscriptions and other publications that cover a wide range of subjects related to technology research. We also use the extensive library of directories and Journals on various technology domains. Our analysts use blog posts, whitepapers, case studies, and other literature published by major technology vendors, online experts, and industry news publications.

Inputs from Industry Participants

QKS Group analysts collect relevant documents such as whitepapers, brochures, case studies, price lists, datasheets, and other reports from all major industry participants.

Primary Research

QKS Group analysts use a two-step process for conducting primary research that helps us capture meaningful and accurate market information. Below is the two-step process of our primary research:

Market Estimation: Based on the top-down and bottom-up approach, our analyst analyses all industry participants to estimate their business in the technology market for various market segments. We also seek information and verification of client business performance as part of our primary research interviews or through a detailed market questionnaire. The QKS Group research team conducts a detailed analysis of the comments and inputs provided by the industry participants.

Client Interview: The QKS Group analyst team conducts a detailed telephonic interview of all major industry participants to get their perspectives on the current and future market dynamics. Our analyst also gets their first-hand experience with the vendor's product demo to understand their technical capabilities, user experience, product features, and other aspects. Based on the requirements, QKS Group analysts interview more than one person from each of the market participants to verify the accuracy of the information provided. We typically engage with client personnel in one of the following functions:

- Strategic Marketing Management
- Product Management
- Product Planning
- Planning & Strategy

Feedback from Channel Partners and End Users

QKS Group research team research with various sales channel partners, including distributors, system integrators, and consultants, to understand the detailed perspective of the market. Our analysts also get feedback from end-users from multiple industries and geographical regions to understand key issues, technology trends, and supplier capabilities in the technology market.

SPARK Matrix:
Strategic Performance Assessment and Ranking

QKS Group's SPARK Matrix™ provides a snapshot of the market positioning of the key market participants. SPARK Matrix™ representation provides a visual representation of market participants and provides strategic insights on how each supplier ranks in comparison to their competitors concerning various performance parameters based on the category of technology excellence and customer impact.

Final Report Preparation

After the finalization of the market analysis, our analyst prepares the necessary graphs, charts, and tables to get further insights and prepares the final research report. Our final research report includes information including competitive analysis, major market & technology trends, market drivers, vendor profiles, and others.